REMARKS

This supplemental amendment is filed in response to the office action mailed October 7, 2004.

I. STATUS OF THE CLAIMS

As of the date of this Amendment, claims 1-6 and 9-12, 14-61 remain pending. Claims 4 and 35 have been amended. Claims 1, 3-5, 9, 11, 14, 16, 18, 20, 22, 40, 42-43, 50, 52, 56, and 58 are independent claims.

PART 1 - SUMMARY OF THE ISSUES IN THE PRESENT APPLICATION

I. Introduction

Applicants assert that many of the primary issues (i.e., establishing that publications are actually prior art references, motivation for combining prior art references, etc.) raised in Applicant's previous response of October 14, 2003, which thoroughly rebutted all of the Examiner's objections and rejections, have not been addressed by the Examiner. Applicants further assert that until such time as the Examiner addresses the primary issues raised by Applicants, all of the Examiner's additional, secondary issues raised in the outstanding office action of October 7, 2004, are not ripe for argument.

In an effort to focus prosecution on these key, primary issues, Applicants' offer the following summary. This Summary is followed by Part 2, which specifically addresses the additional, secondary issues in the outstanding office action of October 7, 2004.

II. General Summary of the Present Invention

In a broad, general sense, example embodiments of the present invention are directed to methods and systems of communicating messages cryptographically, which use three or

more random and distinct prime numbers. Claims directed to such example methods include presently pending independent claims 1, 3, 14, 16, 18, 20, 22, and 40. Claims directed to such example systems include presently pending independent claims 4, 5, 9, 11, 42, 43, 50, 52, 56, and 58.

Other example embodiments are directed to methods and systems of communicating messages cryptographically, which develop subtask values corresponding to the message in parallel. Claims directed to such example systems include presently pending dependent claims 44 and 45.

III. Support in the Original Collins et al. Patent for the General Invention

Applicants respectfully submit that column 3, line 27-29 of the original Collins et al. patent recite that it is an object of the present invention to provide a system and method for utilizing "multiple (more than two) distinct prime number components to create n." Further, column 3, lines 40-41 of the original Collins et al. patent recite that "n is developed from three or more distinct prime numbers; i.e., $n = p_1 \cdot p_2 \cdots p_k$, where k is an integer greater than two." Column 5, lines 31-32 recite an example assuming three or more random, large, distinct primes, p_1, p_2, ...p_k. Column 5, lines 66-67 recite an example assuming three distinct primes, p_1, p_2, and p_3. The original abstract also recites "three or more distinct primes.". Accordingly, Applicants respectfully submit that the original Collins et al. patent at least supports claims directed to more than two distinct prime numbers, three distinct prime numbers, three or more distinct prime numbers, and three or more random and distinct prime numbers. Applicants fail to see how the Examiner could conclude otherwise.

IV. Establishing Various, Alleged Prior Art References are In Fact Prior Art

A. U.S. Patent 5,974,151 to Slavin

The Examiner has applied U.S. Patent 5,974,151 to Slavin against several claims of the present application under 35 U.S.C. § 102(a). 35 U.S.C. § 102(a) states:

> A person shall be entitled to a patent unless -
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for patent,...

A cursory inspection of Slavin reveals Slavin was published on October 26, 1999, almost three (3) years after the present application was filed (on January 16, 1997) and almost eleven (11) months after the Collins et al. patent was granted (on December 8, 1998). Applicants are at loss to explain how the Examiner could conclude Slavin is 35 U.S.C. § 102(a) prior art against the present application.

B. "RSA Moduli Should Have 3 Prime Factors" to Captain Nemo

The Examiner has again applied "RSA Moduli Should Have 3 Prime Factors" to Captain Nemo against several claims of the present application under 35 U.S.C. § 103(a). While the exact basis for this rejection is unclear, Applicants assume the basis is under 35 U.S.C. § 102(b). 35 U.S.C. § 102(b) states:

> A person shall be entitled to a patent unless -
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of the application for patent in the United States, ...

Applicants will not further debate the merits of the teachings of Nemo, until the Examiner can establish that Nemo is, in fact, prior art against the present application. Applicants continue to assert that the Examiner has not established that Nemo is, in fact, a publication. The date on which the public actually gained access to Nemo is the relevant date.

On its face, Nemo states that it was published in "Scientific Bulgarian" magazine in August 1996. Applicants have checked the existence of "Scientific Bulgarian" magazine and have concluded that a paper form of an "August 1996" issue (or any other paper issue containing Nemo) was never produced or made available to the public. If the Examiner can establish otherwise, he is invited to do so. If not, he should withdraw all rejections relying on Nemo.

Applicants have further checked the Internet for any credible evidence of the presence of an electronic copy of Nemo available to the public via the Internet prior to the filing date of the present application and have concluded that Nemo was also not available in electronic form. If the Examiner can establish otherwise, he is invited to do so. If not, he should withdraw all rejections relying on Nemo.

Finally, Applicants conducted a quick and rudimentary search of the U.S.P.T.O's patent database (at www.uspto.gov) from 1976 to the present and have discovered that not one issued U.S. patent in that time period lists Nemo or any other article from any other issue of "Scientific Bulgarian" magazine as a prior art publication.

V. The Teachings of Various Prior Art References With Respect to "Three or More Random and Distinct Prime Numbers"

A. General

The Examiner has asserted that several prior art references teach three or more random and distinct prime numbers without ever specifically setting forth such a teaching. Applicants find this rationale particularly confusing when contrasted with the Examiner's position that the present application, which specifically refers to "three or more random and distinct prime numbers" at col. 5, lines 31-32, does not teach "three or more random and distinct prime numbers". Applicants will address each of these references individually below.

B. U.S. Patent 4,405,829 to Rivest et al (RSA)

RSA teaches two or more distinct primes. Nowhere does RSA even mention "random", let alone "random and distinct", let alone "three or more random and distinct prime numbers". Accordingly, Applicants assert RSA fails to teach or suggest "three or more random and distinct prime numbers". Applicants fail to see how the Examiner could conclude otherwise.

C. "A Method for Obtaining Digital Signatures and Public-key Cryptosystems" by Rivest et al. (Rivest)

Rivest teaches two random primes. Nowhere does Rivest even mention "distinct", let alone "random and distinct", let alone "three or more random and distinct prime numbers". Accordingly, Applicants assert Rivest fails to teach or suggest "three or more random and distinct prime numbers". Applicants fail to see how the Examiner could conclude otherwise.

D. The Art of Computer Programming by Knuth (Knuth)

Knuth teaches nothing about prime numbers. Nowhere does Knuth even mention "random", let alone "distinct", let alone "random and distinct", let alone "three or more

random and distinct prime numbers". Accordingly, Applicants assert Knuth fails to teach or suggest "three or more random and distinct prime numbers". Applicants fail to see how the Examiner could conclude otherwise.

E. "Using four-prime RSA in which some bits are Specified" by Vanstone and Zuccherato (Vanstone)

Vanstone teaches four prime numbers. Nowhere does Vanstone even mention "random", let alone "distinct", let alone "random and distinct", let alone "three or more random and distinct prime numbers". Accordingly, Applicants assert Vanstone fails to teach or suggest "three or more random and distinct prime numbers". Applicants fail to see how the Examiner could conclude otherwise.

F. "A Public-Key Cryptosystem Suitable for Digital Multisignatures" by Itakura and Nakamura (Itakura)

Itakura teaches three prime numbers. Nowhere does Itakura even mention "random", let alone "distinct", let alone "random and distinct", let alone "three or more random and distinct prime numbers". Accordingly, Applicants assert Itakura fails to teach or suggest "three or more random and distinct prime numbers". Applicants fail to see how the Examiner could conclude otherwise.

VI. Motivation for Combining Various Prior Art References

A. General

It is apparent that in the above section, applicants have taken each valid prior art reference separately and compared it to a broad characterization of the present invention, a broad characterization which is present in each and every independent claim. A proper analysis does not conclude with a discussion of the teachings of the prior art references

individually, especially in a § 103 rejection. Of course, to establish a § 103 rejection, it is impermissible for an Examiner to pick and choose various teachings of the prior art references, in order to piece together the invention recited in the claims to be rejected.

In Applicants' prior response of October 14, 2003, Applicants challenged the Examiner's motivation for combining RSA, Rivest, and Knuth. In the outstanding office action of October 7, 2004, which includes 68 paragraphs over 25 pages (and raises scores of secondary issues, all tangential to the primary issues laid out above), the Examiner devotes a total of one sentence to motivation. The sentence in question can be found on page 23, at the end of paragraph 67, where the Examiner, apparently trying to establish motivation for combining RSA and Rivest, states:

> "The motivation for distinct randomly choosen (sic) distinct multiprime comes from the same authors and thus is not pieced together."

Applicants are aware of no valid, current, U.S. patent decision which has held that two publications by one author or inventor or one set of authors or inventors, is per se, combinable under 35 U.S.C. § 103(a). In fact, in at least *In re Kotzab*, 217 F.3d 1365, 55 USPQ2d 1313 (Fed. Cir. 2000), the CAFC held that even separate embodiments of the same patent cannot be combined absent some motivation to do so.[1]

B. RSA and Rivest

As set forth above, the mere fact that two publications are from the same author(s) or inventor(s) is not sufficient motivation to combine them. Accordingly, Applicants submit that the Examiner has not set forth any reasons why one of ordinary skill in the art would pick and choose various teachings of RSA and Rivest in order to piece together the invention

recited in the presently pending claims. Applicants respectfully request the Examiner to supply proper motivation or withdraw the rejection.

C. RSA and Knuth

Applicants submit that the Examiner has not set forth any reasons why one of ordinary skill in the art would pick and choose various teachings of RSA and Knuth in order to piece together the invention recited in the presently pending claims. Applicants respectfully request the Examiner to supply proper motivation or withdraw the rejection.

D. Rivest and Knuth

Applicants submit that the Examiner has not set forth any reasons why one of ordinary skill in the art would pick and choose various teachings of Rivest and Knuth in order to piece together the invention recited in the presently pending claims. Applicants respectfully request the Examiner to supply proper motivation or withdraw the rejection.

E. Itakura and Rivest

Applicants submit that the Examiner has not set forth any reasons why one of ordinary skill in the art would pick and choose various teachings of Itakura and Rivest in order to piece together the invention recited in the presently pending claims. Applicants respectfully request the Examiner to supply proper motivation or withdraw the rejection.

PART 2 - OTHER ISSUES RAISED IN THE OUTSTANDING OFFICE ACTION OF OCTOBER 7, 2004

[1] The Examiner's argument in paragraph 23 is also contrary to the holding of *Katzab*.

I. OBJECTION TO THE SPECIFICATION – NEW MATTER

Sections 1-6 and 61-66 of the outstanding office action of October 7, 2003, indicate that Applicants' previous amendment of October 14, 2003 has been objected to under 35 U.S.C. § 132 as having allegedly introduced new matter into the specification.

In Sections 2 and 63, the Examiner objects to the replacement of the term "using" with the term "extending". Applicants assert that the conventional RSA scheme uses two primes, whereas the present invention uses three or more. In this context, Applicants believe that the present invention "extends" the number of primes from two to three or more. As a result, Applicants believe that the present invention "extends" the RSA scheme. Accordingly, reconsideration and withdrawal of the objection is respectfully requested.

In Sections 3 and 64, the Examiner asserts that the change that "three or more random large, distinct primed numbers are developed and checked to ensure that each (p_i-1) is relatively prime to e" is new matter.

Applicants direct the Examiner's attention to originally filed independent claim 1, filed on January 16, 1997 which recites e is a number relatively prime to $(p_1-1) \cdot (p_2-1) \cdot \ldots (p_k-1)$. Accordingly, Applicants respectfully submit that the change to column 5, lines 31-33, merely brings the specification into compliance with original claim 1. Further, Applicants respectfully submit that one of ordinary skill in the art would recognize that the equation recited at column 5, line 39 would not work if three or more random large distinct prime numbers were not relatively prime to e. Accordingly, reconsideration and withdrawal of this rejection is respectfully requested.

In Sections 4 and 62, the Examiner asserts that the amendment to column 5, line 52, to add a digital signature, is not supported. However, Applicants have been unable to locate the addition of a "digital signature" in Applicants previous response. Clarification of this rejection is requested.

In Sections 5 and 64, the Examiner asserts that the amendment to the specification to column 6, line 24 to change "$i \geq 2$" to "$2 \leq i \leq k$ where k is the number of primes in n" constitutes new matter.

Applicants respectfully submit that this change merely more accurately recites the teachings of the present invention. As set forth clearly throughout the specification, there are no prime numbers beyond p_k; accordingly, it makes absolutely no sense to indicate prime numbers greater than equal to 2, but unbounded by the number of prime numbers k. Accordingly, Applicants respectfully submit that this is not new matter, but merely a reflection of the upper bound of the number of k primes, which the change of which, Applicants believe more accurately represents the present invention. However, although less accurate, Applicants are willing to leave this portion of the specification as "$i \geq 2$".

In Section 6, with regard to column 6, line 65, the Examiner asserts that the change from "the decrypted message M can be obtained" to "the ciphertext C can be obtained" is new matter. The Examiner further asserts that in the first version, summation is required, wherein the second version iteration is required.

In response to this objection, Applicants respectfully submit that there are at least two know solutions for the Chinese Remainder Theorem. The first, proposed by Gauss, is a summation technique, and therefore not recursive. The second, proposed by Garner, is a recursive technique. Applicants respectfully submit that the original patent describes Garner's technique beginning at column 6, line 1 and Gauss' technique, beginning at column 7, line 1. Since the present application supports both recursive and non-recursive solutions, Applicants assert that the Amendment to column 6, line 65 does not constitute new matter.

II. CLAIM OBJECTIONS

In Sections 7 and 8, the Examiner points out minor informalities in the previous amendments to claims 4 and 35. Applicants have amended claims 4 and 35 to correct these minor informalities.

III. CLAIM REJECTIONS UNDER 35 U.S.C. § 112

A. 35 U.S.C. § 112, FIRST PARAGRAPH

In Section 10, claim 1 is rejected under 35 U.S.C. § 112, first paragraph but no specific rejection is set forth. Applicants assume this rejection is related to the objection to the specification under 35 U.S.C. § 132 and therefore traversed for the reasons set forth above.

In Sections 11 and 12, the Examiner asserts that claims 1-2, 18-19, 32-33, 37, 42-49, and 56-61 are rejected under 35 U.S.C. § 112, first paragraph, because the patent as originally filed does not disclose $k \geq 3$. Applicants respectfully submit that column 3, line 27-29 of the original Collins et al. patent recite that it is an object of the present invention is to provide a system and method for utilizing "multiple (more than two) distinct prime number components to create n." Further, column 3, lines 40-41 of the original Collins et al. patent recite that "n is developed from three or more distinct prime numbers; i.e., $n = p_1 \cdot p_2 \cdot \ldots p_k$, where k is an integer greater than two." Finally, column 5, lines 66-67 recite an example assuming three distinct primes, p_1, p_2, and p_3. Accordingly, Applicants respectfully submit that an amendment reciting k is an integer greater than two is supported by multiple passages in the original Collins et al. patent.

In Sections 13-15, the Examiner asserts that claims 1-61 are rejected under 35 U.S.C. § 112, first paragraph, objecting to the term "random". The Examiner correctly points out that the term random is utilized in the original patent at column 5, line 31 and is therefore

supported by the original patent. Applicants assert that this disclosure supports the claims as amended.

In Applicants previous Response, Applicants asserted that "the randomness and distinctness attributes of the k prime numbers will materially improve the security in any cryptographic system with RSA public key encryption".

With respect to this statement, the Examiner asserts that if this were the intent of the original patent, the original patent does not support this view. Applicants respectfully submit that the above statement is an advantage of the present invention. Advantages of the present invention need not be provided in the specification In re Chu, 36 U.S.P.Q.2d 1089 (Fed.Cir. 1995). Accordingly, Applicants respectfully submit that claims 1-61 are supported by the original specification, because random is provided in the original patent, and any purported advantage of the randomness need not be present in the original patent.

B. 35 U.S.C. 112, SECOND PARAGRAPH

In Section 18, the Examiner objects to amended claim 9, specifically the word "means" is not followed by a function. Applicants have reviewed claim 9 and are unsure of the Examiner's rejection, in particular, each means clause of claim 9 appears to recite a function.

IV. CLAIM REJECTIONS UNDER 35 U.S.C. § 103

In sections 19-49 and 67 of the Office Action, claims 1-7, 9-61 are rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent 4,405,829 to Rivest et al., (RSA), and further in view of Rivest et al. "A Method for Obtaining Digital Signatures and Public-key Cryptosystem", Communications of the ACM, 21(2) February 1978, (Rivest) and further in view of Knuth, The Art of Computer Programming Vol. 2, page 179 (Knuth).

This rejection is respectfully traversed for the reasons set forth above in Part 1, Sections V-A through V-D and Sections VI-A through VI-D, and for the reasons set forth in Applicants' previous response of October 14, 2003.

In Sections 53 and 60, claims 1-6, 9-12, 14-31, 34-36, 38-44, and 50-61 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Nemo (RSA Moduli Should Have 3 Prime Factors) (Nemo), and further in view of Rivest.

This rejection is respectfully traversed for the reasons set forth above in Part 1, Section IV-B, Section V-A, and Section VI-A, and for the reasons set forth in Applicants' previous response of October 14, 2003.

In Section 56, claims 1-6, 11-12, 14-17, 20-31, 34-36, 38-44, and 50-61 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Itakura and Nakamura, A Public-Key Cryptosystem Suitable for Digital Multisignatures, NEC Res. & Develop. No. 71, October (Itakura), and further in view of Rivest.

This rejection is respectfully traversed for the reasons set forth above in Part 1, Sections V-A and V-F and Sections VI-A and VI-E, and for the reasons set forth in Applicants' previous response of October 14, 2003.

V. CLAIM REJECTION UNDER 35 U.S.C. § 102

In Sections 50-52 and 68, claims 1-6, 11-12, 14-17, 20-31, 34-36, 38-44, 50-57, 60-61 are rejected under 35 U.S.C. § 102(b) as being anticipated by Vanstone and Zuccherato, "Using four-prime RSA in which some bits are Specified", Electronic Letters, 30(25), 16 August 1994, (Vanstone).

This rejection is respectfully traversed for the reasons set forth above in Part 1, Sections V-A and V-E, and for the reasons set forth in Applicants' previous response of October 14, 2003.

In Sections 58, claims 1-6, 9-12, 14-31, 34-36, 38-44, and 50-61 are rejected under 35 U.S.C. § 102(a) as being anticipated by Slavin.

This rejection is respectfully traversed for the reasons set forth above in Part 1, Section IV-A.

CONCLUSION

Accordingly, in view of the above amendments and remarks, reconsideration of the objections and rejections and allowance of each of claims 1-6, 9-12, and 14-61 in connection with the present application is earnestly solicited.

Pursuant to 37 C.F.R. §§ 1.17 and 1.136(a), Applicant(s) hereby petition(s) for a one (1) one month extension of time for filing a reply to the outstanding Office Action. The fee for extension fee of $120 is being paid herewith. Should there be any outstanding matters that need to be resolved in the present application, the Examiner is respectfully requested to contact John A. Castellano at the telephone number of the undersigned below.

If necessary, the Commissioner is hereby authorized in this, concurrent, and future replies, to charge payment or credit any overpayment to Deposit Account No. 08-2025 for any additional fees required under 37 C.F.R. § 1.16 or under 37 C.F.R. § 1.17; particularly, extension of time fees.

Respectfully submitted,

HARNESS, DICKEY, & PIERCE, P.L.C.

By _____

John A. Castellano, Reg. No. 35,094
P.O. Box 8910
Reston, Virginia 20195
(703) 668-8000

JAC/pjd

CERTIFICATE OF SERVICE

I hereby certify that a true copy of the Supplemental Amendment filed concurrently herewith, was served via first class mail, this 25th day of March, 2005 to:

Patent Administrator
Testa, Hurwitz & Thibeault, LLP
125 High Street
Boston, Massachusetts 02110

John A. Castellano, Esquire